PATENT ABSTRACTS OF JAPAN

(11) Publication number:

11215122 A

(43) Date of publication of application: 06.08.99

(51) Int. CI

H04L 9/36

G09C 1/00

(21) Application number: 10013727

(71) Applicant:

MATSUSHITA ELECTRIC IND CO

LTD.

(22) Date of filing: 27.01.98

(72) Inventor:

HARADA TOSHIHARU OKUMURA YASUO TATEBAYASHI MAKOTO

SAIJO TAKESHI ONO TAKATOSHI

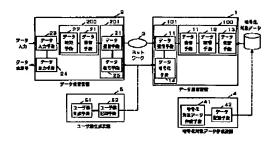
(54) METHOD, DEVICE, AND SYSTEM FOR **ENCIPHERING DATA**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a method, device, and system for enciphering data by which only the necessary scope of data distributed through WWW(world-wide web) can be enciphered in accordance with the contents of the data.

SOLUTION: (1) A data receiver 2 transmits data request information and receiver identification information when a user inputs data required by the user in a WWW browser 200. (2) A data transmitter 1 enciphers the data to be enciphered corresponding to the data requesting information and incorporating an enciphering scope designating instruction within the extent designated by the enciphering scope designating instruction in such a way that only the receiver can decode the enciphered data in an enciphering proxy 101 and transmits the results to the data receiver 2. (3) The data receiver 2 decodes the enciphered data in a decoding proxy 201 and outputs the decoded data.

COPYRIGHT: (C)1999,JPO



2

(11)特許出頭公園番号

特開平11-215122

(43)公開日 平成11年(1999)8月6日

G09C	H04L	(51) Int CL*
1/00	9/36	
660		建 別記号
G09C	H04L	FΙ
1/00	9/00	
660Z	685	

存金組分子 未開次 超泉域の数15 01 (全 19 頁)

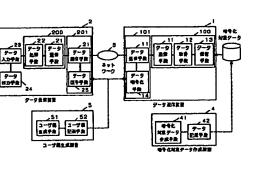
是并耳门较个	建			
	(74)代理人 弁理士 指本 智之 (911名)	(74)代理人 5		
	直蒙株式会社内	ho:		
热下囊器	大阪府門其市大学門真1006番地 松下電器	<u> </u>		
	30 年 13	(72)発明者 #		
	商業株式会社内	her		
松下鐵器	大阪的門其市大学門真1008番地 松下電器			
	英村 康男	(72)発明者 3		
	産業株式会社内	ha.		
松下電器	大阪府門其市大学門其1006番地 松下電器			
	原田後治	(72)発明者 1		
	大阪府門其市大学門真1008番地	<u> </u>	平成10年(1998) 1月27日	(22)出版日
	松下電器産業株式会社	-		
	00005821	(71)出版人 000005821	特別 平10-13727	(21)出國籍中

(54) 【発明の名称】 データ暗号方法、データ暗号装置、及びデータ暗号システム

(57) 【聚学】

ステムを提供する。 に応じて必要な範囲だけを暗号化する方法、装置及びに 【課題】 WMVで配信されるデータに対して、その内容

る。(2)データ送信校の1は、時号プロキシ101にお けとると、データ要求情報と受信者識別情報を送信す 泉データを復号し、復号されたデータを出力する。 は、復身プロキシ201において四号化された四号化対 データ受信装置2に送信する。(3)データ受信装置2 れた受信者のみが復身できるように暗身化しこの結果を 指定命令で指定された復聞を、受信者類別指棋で指定さ が組み込まれた時号化対象データに対して、時号化鏡囲 いて、アータ既求始報に対応した、昭号化徳囲指院命令 00において、ユーザから取得したいデータの入力を必 【解決手段】 (1)データ受信校団 2 は、WMプラウザ;



【特許請求の範囲】

を行なうデータ暗号方法であって、 組み込まれた命令に従って暗号化処理を含むデータ処理 定する命令が組み込まれた暗号化対象データに対して、 【請求項1】暗号化処理方法を含むデータ処理方法を指

命令で指定された範囲を暗号化することを特徴とするテ **時号化する範囲を指定する暗号化範囲指定命令が組み込** 一夕暗号方法。 まれた暗号化対象データに対して、前記暗号化範囲指定

を暗号化するようにしたことを特徴とする酵水項1記録 のうち、前記時号化範囲指定命令により指定された範囲 **強に対応する暗号化鍵を用いて、前記暗号化対象データ** 前記受信者指定命令で指定された受信者が保持する很易 定する受信者指定命令が狙み込まれている場合に、 指定命令に加えて、前起暗号化対象データの受信者を指 【請求項2】前記暗号化対象データに、前記暗号化範囲

のデータ暗号方法。

号化された前記第1の復号鍵を指定する鍵情報指定命令 信者の保持する第2の復号観に対応する第2の暗号化観 を組み込んだ暗号化データを得るようにしたことを特質 で暗号化し、暗号化された前記暗号化対象データに、暗 し、前記第1の暗号化鍵に対応する第1の復号鍵を、受 とする請求項1記載のデータ暗号方法。 し、前記略号化対象データを募1の暗号化銀で暗号化 【請求項3】前記略号化対象データを暗号化するに際

データ暗号方法であって、 まれた命令に従って復号処理を含むデータ処理を行なう する命令が組み込まれた暗号化データに対して、組み込 【請求項4】彼号処理方法を含むデータ処理方法を指定

復号する範囲を指定する復号範囲指定命令が狙み込まれ された範囲を復号することを特徴とするデータ暗号方 た母中代データに対して、歯蛇彼や徳囲指に命令で指に

定命令が狙み込まれている場合に、 令に加えて、暗号化データの受信者を指定する受信者指 【訪求項5】前記略号化データに、前記復号範囲指定命

前記受信者指定命令で指定された受信者が保持する役号 号するようにしたことを特徴とする請求項4記載のデー 指定命令により指定された範囲を前記復号鍵を用いて復 鍵を用いて、前記暗号化データに対して、前記復号範囲

題情報指定命令が組み込まれている場合に、 令に加えて、暗号化された前記第1の復号器を指定する 【緯求項6】前記略号化データに、前記復号範囲指定命

者の保持する第2の復号鍵で、復号し、 前記吗号化データを復号するに際し、前記銀竹報指定角 合で指定された暗号化された前記第1の復号鍵を、受信

鍵を用いて復号するようにしたことを特徴とする請求項 前記役号範囲指定命令により指定された範囲を前記復号 前記暗号化データを、復号された前記第1の復号観で、

4 記載のデータ暗号方法。

定用の命令を利用し、そのコメントとしてあらかじめ定 みなすようにしたことを特徴とする請求項1から6のう ための命令群の中から対応する命令が指定されたものと 令、前記受信者指定命令、及び、前記録情報指定命令の 指力いた命令である場合に、原号処理のたろの命令群、 が、特に、HTML(Hypertext Warkup Language)腎語に ちいずれか1項記載のデータ暗号方法。 めた特定のコメントが指定された時に前述の既号処理の 記述方法として、前記HDALで危殺されているコメント的 すなわち前記暗号化範囲指定命令、前記復号範囲指定命 【請求項7】前記啞号化対象データに組み込まれる命令

を行なうデータ時号数置であって、データ通信手段と、 組み込まれた命令に従って暗号化処理を含むデータ処理 定する命令が狙み込まれた暗号化対象データに対して、 データ収得手段と、データ保管手段と、データ暗号化手 【請求項8】暗号化処理方法を含むデータ処理方法を指

た時号化対象データの送信を要求するデータ要求情報を 化データを作成し、データ通信手段が、前記暗号化デー された範囲を暗号化し、この結果として得られる少なく 管手段から取得し、前記データ晴号化手段が、前記暗号 何報で要求された前記略号化対象データを前記データ保 受信したとき、前記データ取得手段が、前記データ要求 前記データ通信手段が、前記データ保管手段に保管され とするデータ暗号装置。 する範囲を指定する彼号範囲指定命令を削み込んだ暗号 とも一部が暗号化された前記暗号化対象データに、復号 化対象データのうち前記暦号化模囲指定命令により指定 タを前記データ要求情報の発信元に送信することを特別

昭号化手段を有する暗号化プログラムとが実装されたコ 段を備えたWYM(World Wide Web)サーバと、前記データ ンピュータであることを特徴とする耐水項8記載のデー 通信手段と、前記データ取得手段と、前記データ保管手 夕晒号装伍。 【蔚永項9】前記データ暗号装置が、特に、前記データ

を行うためのデータ通信手段を有するプログラムである 記略号化対象データもしくは前記略号化データの遊受信 号化手段に加えて、MMサーバまたはMMブラウザと、前 ことを特徴とする助求項9記載のデータ略号装成。 【蔚永項10】前記暗号化プログラムが、前記データ暗

一タ復号手段を備え、 処理手段と、データ入力手段と、データ出力手段と、デ **うデータ暗号装置であって、データ通信手段と、デー** 込まれた命令に従って很号処理を含むデータ処理を行な 定する命令が組み込まれた時号化データに対して、組み 【請求項11】 後号処理方法を含むデータ処理方法を指

前記データ入力手段に、外部から取得したい暗号化対象 信手段が、前記略号化対象データの送信を要求するデー データを指定する情報が入力されたとき、前記データ通

タ 要求情報を送信し、前記データ要求情報に対応する、 復号する範囲を指定する復号範囲指定命令が組み込まれ た時号化データを受信し、前記データ復号手段が、前記 時号化データのうち復号範囲指定命令で指定された範囲 を復号し、前記データ処理手段が、復号された時号化デ ータを、ディスプレやブリンタなどのデータ出力数度が 接続された前記データ出力手段に出力することを特徴と するデータ時号数面。

【閉求項12】 放記データ受包装係が、特に、放記データ通信手段と、放記データ処理手段と、放記データ人力手段と、放記データと型手段と、放記データ人力手段と、放記データ担力手段を相えたMMVブラウザと、 放記データ提号手段を有する担号プログラムが実装されたコンピュータであることを特徴とする耐求項11記載のデータ項号数回。

【協求項13】前記彼号プログラムが、前記データ復号手段に加えて、mWサーバまたはmWプラウザと、 請記呼号化対象データもしくは描記呼号化データの送季

は記時号化対象データもしくは前記時号化データの送受信を行うためのデータ通信手段を有するプログラムであることを特徴とする時収到12記載のデータ暗号数配。 【仰沢川14】データ通信手段と、データ収得手段と、データ保管手段と、データ場号に乗及と、データ場で手段と、データ保管手段と、データ場合手段と、ユーザ酸保管手段とを備えた送信頭のデータ明号表配と、

データ通信手段と、データ処理手段と、データ入力手段と、データ出力手段と、データ出力手段と、データ復号手段と、ユーザ段保管手段とを増えた受信頭のデータ時号装置と、キットワークと、暗号化対象データ作成手段と暗号化対

泉データ配送手段を備えた暗号化対象データ作成装取

ユーザ鹿生成手段とユーザ鹿配送手段を備えたユーザ鹿生成数位とで構成されるデータ晒号システムであって、前記ユーザ鹿生成数位において、前記ユーザ鹿生成手段が、谷ユーザ周右の晒号化融とこの晒号化融に対応する後号銀を生成し、前記ユーザ鹿配送手段が、前記暗号化銀を前記送信間のデータ暗号数位のユーザ鹿保管手段に保管し、前記復号路を前記受信舗のデータ時号效位のユーザ鹿保管手段に保管し、前記復号路を前記受信舗のデータ時号效位のユーザ鹿保管手段に保管し、

前記時号化対象データ作成院間において、前記時号化対象データ作成手段が、時号化する範囲を指定する時号化範囲指定命令を組み込んだ時号化対象データを作成し、前記時号化対象データ配送手段が、前記時号化対象データを前記送信頭のデータ時号数回のデータ保管手段に保容し、

前配会信頼のデータ時号数配において、前記データ入力 手段に、外部から取得したい時号化対象データを指定する情報が入力されたとき、前記データ通信手段が、前記 時号化対象データの送信を要求するデータ要求情報を前 記述信題のデータ時号数配に前記ネットワークを利用して述信し、

前記送信仰のデータ時号校原において、前記データ通信 手段が、前記データ保管手段に保管された時号化対象デ

一夕の遠信を要求するデーク要求信頼を受信したとき、前記デーク取得手段が、前記デーク要求情報を受求された前記時号化対象デークを前記データ展替手段から取得し、前記デーク略号化対象データを前記データに対象データの一方的記略号化模型指定命令により指定された範囲を暗号化し、この結果として得られる少なくとも一郎が唱号化された前記略号化対象データに、復号する範囲を指定する複号範囲指定命令を組み込んだ略号化データを情記を目にデータが同手段が、前記略号化データを前記受信息のデータ通信手段が、前記略号化データを利用して送信のデータ時号表置に前記ネットワークを利用して送信

対記受信間のデータ暗号装置において、前記暗号化データを受信し、前記データ復号手段が、前記暗号化データのうち復号範囲指定命令で指定された範囲を復号し、前記データ処理手段が、復号された暗号化データを、ディスプレやプリンタなどのデータ出力装置が接続された前記データ出力手段に出力することを特徴とするデータ暗号システム。

【請求項15】データ通信手段と、データ取得手段と、データ保管手段とを備えた送信師のデータ暗号数配と、データ通信手段と、データ処理手段と、データ入力手段と、データ出力手段と、データ出力手段と、データ出力手段と、データ出力手段と、データ出力手段と、データ出力手段と、データは号表配と、ネットワークと、

昭号化対象データ作成手段と、データ暗号化手段と、ユーザ線保管手段と、暗号化データ配送手段を備えた暗号 ーザ線保管手段と、暗号化データ配送手段を備えた暗号 化データ作成数阻と、

ユーザ鍵生成手段とユーザ酸配送手段を備えたユーザ酸 生成技面とで構成されるデータ時号システムであって、 前記ユーザ鍵生成数回において、前記ユーザ鍵生成手段 が、各ユーザ固有の暗号化鍵とこの暗号化度に対応する 役号鍵を生成し、前記ユーザ鍵配送手段が、前記四号化 鍵を前記唱号化データ作成数回のユーザ鍵段管手段に保 管し、前記短号鍵を前記受信頃のデータ暗号装回のユーザ鍵保管手段に保管し、前記短号鍵を前記受信頃のデータ暗号装回のユーザ鍵保管手段に保管し、

前記時号化データ作政教園において、前記時号化データ 作政手段が、時号化する範囲を指定する時号化範囲指定 命令を担み込んだ時号化対象データを作成し、前記デー 夕時号化手段が、前記時号化対象データのうち前記時号 化範囲指定命令により指定された範囲を時号化し、この 結果として得られる少なくとも一部が暗号化された前記 時号化対象データに、接号する範囲を指定する後号範囲 指定命令を組み込んだ時号化データを作成し、前記時号 化データ配送手段が、前記時号化データを伸起返信頭の データ暗号数回のデータ保管手段に保管し、

前記受信調のデータ暗号装置において、前記データ入力手段に、外部から取得したい暗号化対象データを指定する情報が入力されたとき、前記データ通信手段が、前記暗号化データの送信を要求するデータ要求情報を前記送信側のデータ暗号装置に前記ネットワークを利用して送

前記送信題のテータ暗号装置において、前起データ通信手段が、前記データ操作手段に保管された暗号化データの送信を要求するデータ要求情報を受信したとき、前記データ取得手段が、前記データ要求情報で要求された前記時化データを前記データ保管手段から取得し、データ通信手段が、前記暗号化データを前記受信題のデータの通信手段が、前記暗号化データを前記受信題のデータの通信手段が、前記暗号化データを前記受信題のデータを暗記受信題のデータを暗記を信題のデータを暗記を

前記受信週のデータ暗号数度において、前記暗号化データを受信し、前記データ復号手段が、前記暗号化データのうち復号範囲指定命令で指定された範囲を復号し、前記データ処理手段が、復号された暗号化データを、ディスプレやプリンタなどのデータ出力装置が接続された前記データ出力手段に出力することを特徴とするデータ昭号システム。

【発明の詳細な説明】

[1000]

【発明の属する技術分野】略号処理命令を含むデータ処理命令の組み込まれた略号化対象データに対して、組み込まれた命令に従って略号処理を施すための方法、技歴、及びシステムに関する。

[0002]

【従来の技術】WWW(World Wide Teb)システムは、マルチメディア情報の検索や、不特定多数への情報発信といった機能を、非常に関照なユーザインターフェースで設供するため急速に替及している。このため、WWWシステムを、パソコンソフトのオンライン販売など、簡用システムを保険する際のプラットフォームとして利用されつのよる。

[0003] MNIシステムを利用して発信される有料の 電子情報や、筋外移の電子情報(以下、単にMNIデータ と称する)を、特定の受信者以外に盗聴(露見)されないようにするために、MNIデータを暗号化することが考えられる。また、特に商用利用の場合は、MNIデータを、その内容に応じて、一部を規範可能とし、重要な組分だけを暗号化するといった、きめ細かく暗号化することが考えられる。

[0004] 従来、WWシステムで発信する電子情報を 暗号化する方法としては、NetscapcCommunications社が 提唱するSSL(Secure Socket Layer)や Enterprise Inte gration Technologies社が提唱するS-HTIPがあり、これ らを用いるとWWデータは暗号化されるため第三者への 盗聴(35見)を防止することができる。なお、SSL及US -HTIPについては、何えば、Q出版社のOPEN DESIGN、19 96年6月号(依7度)を参照されたい。

[0005

【袋明が解決しようとする課題】しかしながら、これらの能来方法は、いずれも、8mmデータを発信するmmサーバと、mmデータを受信するmmプラウザ間で伝送されるmmデータを受信するmmデータを保に対して一致的に暗号化するものであっ

た。このため、MMTデータの内容に応じて、一部はすべた。このため、MMTデータの内容に応じて、一部はすべての受留者に包裹を可能とし、血要を部分だけを時勢化等を作うとき、前記
たとき、前記
た、従来方法では、上述のSSLまたはS-HTTPに基づく時 号機能が追加された専用のMMサーバ及びMMTデラウザが受得し、デー
の要であった。そして、何えば、SSLに基づく時号機能が追加されたMMTデラウザとの両でのみ、MMTデータの時号過能であった。

【0006】本発明は、上記能染の問題点に整み、mmデータを暗号化するに際し、データの内容に応じて、必要を範囲だけを呼号化でき、また、必要であればあらかじめ指定した受信者のみが損号できるようにmmデータを暗号化することも可能とする、データの暗号方法、終 個及びシステムを提供することを第1の目的とする。 【0007】また、既存のmmサーバやmmブラッギに暗号機能を追加する必要のない、すなわち、本発明のデータ暗号化方法に基づく暗号機能が追加された期のmmサーバやmmブラッギを必要としない、データの暗号化方法、银号方法、暗号通信方法、及び、その発度及びシステムを提供することを第2の目的とする。

[8000]

【課題を解決するための手段】上記目のを通成するために、本発明は、暗号化処理方法を含むデータ処理方法を拾定する命令が組み込まれた暗号化対象データに対して、組み込まれた命令に従って暗号化処理を含むデータ処理を行なうデータ暗号方法であって、暗号化する範囲を指定する暗号化範囲指定命令が組み込まれた暗号化対象データに対して、前記時号化範囲指定命令で指定された範囲を暗号化する手段を備える。

【0009】また、前記時号化対象データに、前記時号化超級データに、前記時号化対象データの受信者を指定する受信者指定命令が組み込まれている場合に、前記受信者指定命令で指定された受信者が保持する役号銀に対応する時号化理を用いて、前記時号化対象データのうち、前記時号化競別指定命令により指定された範囲を時号化する手段を備える。

[0010]また、前記時号化対象データを町号化するに際し、前記時号化対象データを新1の暗号化歴で暗号化し、前記期1の暗号化歴に対応する第1の領号歴を、代し、前記期1の暗号化歴に対応する第2の時号化と、受情者の保持する第2の領号を出た当た首記順号化対象データに、歴号化された前記順号化対象データに、暗号化された前記第1の領号服を指定する限情報指定命令を組み込んだ暗号化データを得る手段を備える。

(0011)また、復号処理方法を含むデータ処理方法を指定する命令が組み込まれた時号化データに対して、超み込まれた命令に従って復号処理を含むデータ処理を行なうデータ時号方法であって、復号する範囲を指定する複号範囲指定命令が組み込まれた時号化データに対して、前記復号範囲指定命令で指定された範囲を復号する

手段を悩える。

兒命令で指定された受信者が保持する很号鍵を用いて、 **指定命令に加えて、略号化テータの受信者を指定する受** 前院略号化データに対して、前記徴号範囲指定命令によ 信者指定命令が狙み込まれている場合に、前記受信者指 り指定された範囲を前記領号題を用いて領号する手段を 【0012】また、前記暗号化データに、前記很号範囲

時号化データを復身するに際し、前記鍵情報指定命令で 定する観情報指定命令が狙み込まれている場合に、前記 指定命令に加えて、暗号化された前記第1の復号壁を指 保持する第2の復号歴で、復号し、前記暗号化データ 指定された時号化された前記第1の復号題を、受信者の 【0013】また、前記時号化データに、前記復号範囲

命令により指定された範囲を前記復号数を用いて復号す を、復号された前記第1の復号観で、前記復号範囲指定 る手段を備える。

のとみなすようにする。 理のための命令師の中から対応する命令が指定されたも め始めた特定のロメントが指定された時に前述の暗写風 始命令、前記受信者指定命令、及U、前記聲情報指定命 群、すなわち前記略号化範囲指定命令、前記彼号範囲指 語に指力いた命令である場合に、時号処理のための命令 る命令が、特に、HTML(Hypertext Markup Language) 哲 今の記述方法として、前記HTMLで完成されているコメン ト指定用の命令を利用し、そのコメントとしてあらかじ 【0014】また、前記町号化対象データに組み込まれ

法を指定する命令が狙み込まれた暗号化対象データに対 管手段に保管された時号化対象データの送信を要求する 号化手段を備え、前記データ通信手段が、前記データ保 段と、データ取得手段と、データ保管手段と、データ原 して、組み込まれた命令に従って昭号化処理を含むデー データ要求情報を受償したとき、前記データ取得手段 タ処理を行なうデータ時号炎田であって、データ通信手 【0015】また、暗号化処理方法を含むデータ処理方

が、前記データ要求情報で要求された前記暗号化対象デ 対象データに、後号する範囲を指定する復号範囲指定命 化手段が、前記暗号化対象データのうち前記暗号化範囲 ータを前記データ保管手段から取得し、前記データ暗号 が、前起暗号化データを前記データ要求情報の発信元に 令を狙み込んだ暗号化データを作成し、データ通信手段 して母のれる少なくとも一類が概号化された何哲母母化 指定命令により指定された英囲を辱号化し、この結果と

データ通信手段と、前記データ取得手段と、前記データ れたコンピュータである。 データ暗号化手段を有する暗号化プログラムとが実装さ 保管手段を備えたWMV(World Wide Web)サーバと、前記 【0016】また、前記データ暗号装匠が、特に、前記

【0017】また、前記略号化プログラムが、前記デー

送受信を行うためのデータ通信手段を有するプログラム と、前記時号化対象データもしくは前記時号化データの 夕略号化手段に加えて、WMサーバまたはWMプラウザ

前記データ復号手段が、前記略号化データのうち復号範 号範囲指定命令が組み込まれた暗号化データを受債し、 力されたとき、前記データ通信手段が、前記暗号化対象 と、データ復号手段を備え、前記データ入力手段に、外 行なうデータ暗号装置であって、データ通信手段と、デ 組み込まれた命令に従って復号処理を含むデータ処理を を指定する命令が組み込まれた暗号化データに対して、 ンタなどのデータ出力装置が接続された前記データ出力 手段が、復号された暗号化データを、ディスプレやプリ 囲指定命令で指定された範囲を復号し、前記データ処理 データ要求情報に対応する、彼号する範囲を指定する彼 データの送信を要求するデータ要求情報を送信し、前記 部から取得したい暗号化対象データを指定する情報が入 ータ処理手段と、データ入力手段と、データ出力手段 【0018】また、復号処理方法を含むデータ処理方法

データ通信手段と、前記データ処理手段と、前記データ されたコンピュータである。 と、前記データ復号手段を有する復号プログラムが実装 入力手段と、前記データ出力手段を備えたWMプラウザ 【0019】また、前記データ受信装置が、特に、前記

記略号化対象データもしくは前記略号化データの送受相 復号手段に加えて、MMサーバまたはMMプラウザと、前 を行うためのデータ通信手段を有するプログラムであ 【0020】また、前記復号プログラムが、前記データ

歴生成装置において、前記ユーザ歴生成手段が、各ユー を指定する時号化範囲指定命令を組み込んだ時号化対象 て、前記時号化対象データ作成手段が、暗号化する範囲 信仰のデータ暗号装置のユーザ盤保管手段に保管し、前 成し、前記ユーザ鑑配送手段が、前記暗号化銀を前記送 ザ固有の暗号化鍵とこの暗号化鍵に対応する彼号鍵を生 で構成されるデータ暗号システムであって、前記ユーサ 成手段とユーザ鍵配送手段を備えたユーザ鍵生成装置と 手段を備えた暗号化対象データ作成装置と、ユーザ鍵生 と、暗号化対象データ作成手段と暗号化対象データ配送 とを備えた受信側のデータ暗号装置と、ネットワーク ータ出力手段と、データ復号手段と、ユーザ鍵保管手段 通信手段と、データ処理手段と、データ入力手段と、デ 保管手段とを備えた送信側のデータ暗号装置と、データ 記略号化対象データを前記送信頼のデータ暗号装置のデ 手段に保管し、前記略号化対象データ作成装置におい 記復号銀を前記受信側のデータ時号装置のユーザ鏝保管 データを作成し、前記昭号化対象データ配送手段が、前 【0021】また、データ通信手段と、データ取得手段 **データ保管手段と、データ暗号化手段と、ユーザ錠**

> などのデータ出力装置が接続された前記データ出力手段 るデータ要求情報を受信したとき、前記データ取得手段 号化対象データを指定する情報が入力されたとき、前記 おいて、前記データ入力手段に、外部から取得したい頃 ータ保管手段に保管し、前記受信館のデータ暗号装置に が、領号された暗号化データを、ディスプレやプリンタ 定命令で指定された範囲を復号し、前記データ処理手段 データ復号手段が、前記暗号化データのうち復号範囲指 夕暗号装置において、前記暗号化データを受信し、前記 前記ネットワークを利用して送信し、前配受信側のデー が、前記略号化データを前記受信側のデータ略号装置に 令を組み込んだ噂号化データを作成し、データ通信手段 対象データに、彼号する範囲を指定する彼号範囲指定命 して得られる少なくとも一部が臨時代された前記略号代 指定命令により指定された範囲を暗号化し、この結果と 化手段が、前記暗号化対象データのうち前記暗号化範囲 ータを前記データ保管手段から取得し、前記データ暗号 が、前記データ要求情報で要求された前記暗号化対象デ 保管手段に保管された暗号化対象データの送信を要求す 略号装置において、前記データ通信手段が、前記デーシ 記ネットワークを利用して送信し、前記送信頼のデータ するデータ要求情報を前記送信頼のデータ暗号装置に前 データ通信手段が、前記暗号化対象データの送信を要求

記ユーザ線配送手段が、前記暗号化鍵を前記暗号化デー 位において、前記ユーザ鍵生成手段が、各ユーザ固有の ユーザ錠配送手段を備えたユーザ鍵生成装置とで構成さ **健保管手段とを備えた受信側のデータ暗号装置と、ネッ** 手段と、データ出力手段と、データ復号手段と、ユーサ と、データ保管手段とを備えた送信側のデータ暗号数値 暗号化データ配送手段が、前記暗号化データを前記送信 時号化範囲指定命令により指定された範囲を暗号化し、 指定命令を組み込んだ暗号化対象データを作成し、前記 前記受信間のデータ暗号装置のユーザ健保管手段に保管 タ作成装置のユーザ盤保管手段に保管し、前記很号鐘を 暗号化鍵とこの暗号化鍵に対応する復号鍵を生成し、前 れるデータ町号システムであって、前記ユーザ健生成数 を聞えた暇号化データ作成装置と、ユーザ健生成手段と 化手段と、ユーザ酸保管手段と、暗号化データ配送手段 側のデータ暗号装置のデータ保管手段に保管し、前記受 範囲指定命令を組み込んだ暗号化データを作成し、前記 前記略号化対象データに、復号する範囲を指定する復号 データ暗号化手段が、前記暗号化対象データのうち前記 し、前記暗号化データ作成装置において、前記暗号化テ トワークと、暗号化対象データ作成手段と、データ暗号 この結果として得られる少なくとも一部が暗号化された ―タ作成手段が、暗号化する範囲を指定する暗号化範囲 【0022】また、データ通信手段と、データ取得手段 データ通信手段と、データ処理手段と、データ入力

> のデータ時号校匠に前記ネットワークを利用して送信 化データの送信を要求するデータ要求情報を前記送信仰 類が入力されたとき、前記データ通信手段が、前記時号 に、外部から取得したい暗号化対象データを指定する情 記受信側のデータ暗号装置において、前記暗号化データ 前記データ取得手段が、前記データ要求情報で要求され ータの送償を要求するデータ要求情報を受償したとき、 通信手段が、前記データ保管手段に保管された暗号化テ し、前記送信側のデータ暗号装置において、前記データ データ出力手段に出力する。 データ処理手段が、復号された暗号化データを、ディス うち彼号範囲指定命令で指定された範囲を復号し、前記 データ通信手段が、前記略号化データを前記受信期のデ た前記時号化データを前記データ保管手段から取得し、 プレやプリンタなどのデータ出力装配が接続された前記 を受信し、前記データ很号手段が、前記暗号化データの - 夕晴号装置に前記ネットワークを利用して送信し、前

text Markup Language)官語に指づいて、各種データ処 バを利用し、また、データを受信するデータ受信装匠と は、データを送信するデータ送信装匠として、WMサー いて、図面を用いて説明する。なお、冬気梅の影韻で 理命令が組み込まれる場合について説明する。 配信されるデータの標準的な記述哲語であるHTAL (Hyper 【0024】また、送信されるデータは、WWサーバで して、MMTプラウザを利用する場合について説明する。 【発明の疾癌の形態】以下に、本発明の疾癌の形態につ

式およびRSA暗号方式については、例えば関本英司客、 昭号方式を利用する場合について説明する。DES町号方 夕融と称する)の暗号化には、RSA暗号方式等の公開題 用し、データの暗号化に利用した暗号化鍵(以下、デー cryption Standard) 略号方式等の共通鏡略号方式を利 「暗号理論入門」共立出版(第3章及び第5章)を参照 [0025] また、データの時分化には、DES (Data En

泉データを暗号化し、得られた暗号化データをデータ受 のデータ)を格納しておき、データ送信装促にて、デー 俗物質に送信し、データ受信物質にて、受信した時身化 **ヶ受信装置からの送信要求に対応して、該当の暗号化対** あらかじめ暗号化対象データ(暗号化されていない平文 データを復号して取得する場合について説明する。 【0026】 (契稿の形態1) まず、データ送信校団に

ある。図1に示すようにデータ暗号通信システムは、デ システム構成の既略について説明する。図1は、本浜施 ータ送信装置1と、データ受信装置2と、これらを接続 の影談におけるデータ国导通信システムの質略構改図で そして、本システムの動作辞細について説明する。 に、本システムで扱うデータの構造について説明する。 【0028】「システムの構成」本実施の形態の全体の

【0027】まず、システム構成について説明し、坎

1 5 1

信餌のデータ暗号装置において、前記データ入力手段

するネットワーク3と、暗号化対象データ作成装置4 と、ユーザ競生成装置5によって構成される。

いる。データ暗号化手段には、図示していないがユーザ 指定命令にて指定された受信者向けに時号化して暗号化 WWWサーバの個えるデータ通信手段11が、WWWサーバと やワークステーションなど) が利用できる。この場合、 ationサーバなど) を実装したコンピュータ (パソコン 鍵を保管するための公開鍵保管手段を備えている。デー データを生成するためのデータ暗号化手段14を備えて 対象データを受信者識別情報もしくは後で述べる受信者 成される暗号化データを取得し、この暗号化データをデ 報を受信しそのデータ要求情報に対応した暗号化データ WMプラウギ四の超単過節プロトコルであるHTTPプロト 手段を備えた、既存のWWW(Norld Nide Neb)サーバ (例 化対象データを保管するデータ保管手段13と、暗号化 ータ通信手段に渡すためのデータ収得手段12と、暗号 ータをデータ暗号化手段14に渡し、その結果として生 をデータ保管手段13から取り出し、この暗号化対象テ らのデータ要求情報及びオプションとして受信者識別常 ロルに枯んいてアータ追信を行う。 えば、Netscape Communications社のNetscape Communic 上記データ通信手段と、データ取得手段と、データ保管 魔生成数位 5 によって生成された各ユーギのユーギ公団 1 と、上記データ要求情報に対応する暗号化対象データ 夕町号化手段14の胖相构政については後で説明する。 をデータ受信数置2に送信するためのデータ通信手段 | 【0029】データ送信装匠1は、データ受信装匠2か 【0030】データ送信装匠1としては、具体的には、

すように、CGIプログラムを利用する場合は、データ送 197サーバに追加するためのプログラム)を利用できる。 teway Interface)プログラム(各種データ処理機能をN ムとして動作する。すなわち、OCIプログラムを利用す 信袋低は、データ暗号化手段を提供するCCIプログラム する場合の構成図を図2 (1) に示す。図2 (1) に示 14の実現方法としては、具体的には、CGI (Common Ga る場合、MMサーバ毎にCCIプログラムを追加する必要カ プログラム 101とWがサーバ100は一体のプログラ 101が組み込まれたWWサーバ100で構成され、CC データ送信数図1を、WWサーバとCCIプログラムで実現 【0031】データ送信数位におけるデータ暗号化手段

信数田の構成図を図2(2)に示す。 ともできる。暗号化プロキシで実現する場合のデータ送 グラム (以下、暗号化プロキシと称する) を利用するこ 化手段14の別の実現方法として、暗号化処理代行プロ 【0032】なお、データ送信装置におけるデータ暗号

パと暗号化プロキシで構成した場合のシステムの全体構 【0033】また、図3に、データ送信装匠をWMサー

【0034】図2 (2) 及び図3に示すように、暗号化

ータ通信手段15を備えた暗号化プロキシ102で構成 プロキシによる構成を利用する場合は、データ送信装置 1は、〒Mサーバ100と、データ暗号化手段14とデ

通信のための標準プロトコルであるHTTPプロトコルに描 夕通信手段15は、WMサーバとWMプラウザ間のデータ **少いてデータ通信を行う。** 【0035】 ここで暗号化プロキシ102におけるデー

動作させることが可能となる。そして、その結果、TVNT シでデータ暗号化手段を追加することも可能となる。 ができ、また、複数のYMTサーバに一つの暗号化プロキ サーバとして既存のMMサーバをそのまま利用すること 化プロキシ102は、それぞれ独立のプログラムとして 【0036】この構成により、MMSサーバ100と暗号

得られる復号された暗号化データに対して、各種データ 号化データを復号して、復号された暗号化データを生成 暗号化データをデータ復号手段に渡し、その結果として ータを受信するためのデータ通信手段21と、受信した 置 1 にデータ要求情報及びオプションとして受信者識別 にデータを出力するためのデータ出力手段24を備えて 印刷などのためにディスプレやプリンタなどの外部装備 ためのデータ入力手段23と、データの表示やデータの の保存やデータの印刷などの処理の指定など)を受ける 劇などの処理)を施すためのデータ処理手段22と、暗 処理(例えばデータの表示、データの保存、データの印 情報を送信し、そのデータ要求情報に対応した暗号化デ タ処理の指定(例えば取得したいデータの指定、データ するためのデータ很号手段23と、ユーザから各種デー 【0037】また、データ受信装置2は、データ送信装

生成装置5によって生成されたユーザ秘密器(このデー 25の詳細構成については後で説明する。 るための公開鍵保管手段を備えている。データ復号手段 夕受信装匠を利用するユーザのユーザ秘密鍵) を保管す 【0038】データ復号手段には、図示していないが組

備えるデータ通信手段21が、IMMサーバとIMMブラウサ r) を実装したコンピュータ (パソコンやワークステー tscape Navigatorや、Microsoft社のInternet Explore 等が接続されている。 できる。またデータ出力手段にはディスプレやプリンタ てデータ通信を行う。また、データ入力手段としては、 国の政争追儺プロトリットもるHTPプロトリテに指力で ションなど)が利用できる。この場合、WMアラウザの のWWTプラウザ(例えば、Netscape Communications社Ne 上記データ通信手段と、データ処処理手段を備えた既存 上記コンピュータの増えるキーボードやマウス枠を利用 [0039] データ受信装置2としては、具体的には、

プラグイン(各種データ処理機能をWMプラウザに追加 25の実現手段としては、具体的には、WMプラウザの 【0040】データ受信装置2におけるデータ彼号手段

> するためのプログラム) を利用することができる。デー は、データ復号手段を提供する復号プラグイン201が 手段の構成図を図2 (3) に示す。図2 (3) に示す』 タ復号手段を、プラダインで実現する場合のデータ復号 **ザと復号プラグインは一体のプログラムとして動作す** 組み込まれたWMアラウザ200で構成され、WMアラウ うに、プラグインを利用する場合は、データ受信装置

Wプラウザ毎にプラグインを追加する必要がある。

手段14の別の実現方法として、復号処理代行プログラ 装置をMMプラウザと復号プロキシで構成した場合のシ 構成図を図2(4)に示す。また、図3に、データ受信 きる。復号プロキシで実現する場合のデータ受信装置の ム(以下、復号プロキシと称する)を利用することもで 【0042】なお、データ受信装置におけるデータ復号

てデータ通信手段21を備えた復号プロキシ202で構 は、MMTプラウザ200と、データ復号手段23に加え ロキシによる構成を採用する場合は、データ受信教団 2 [0043] 図2 (4) 及び図3に示すように、復身プ

データ通信を行う。 ための標準プロトロルであるHLLPプロトコルに提びいた 通信手段は、IMTサーバとIMTプラウザ周のデータ通信の 【0044】ここで復身プロキシ202におけるデータ

号プロキシ202は、それぞれ独立のプログラムとして データ復号手段を追加することも可能となる。 き、また、複数のMMアラウザに一つの復号プロキシで 助作させることが可能となる。そして、その結果、WM ブラゥザとして既存のRMTプラウザがそのまま利用で

データ保管手段13に配送するデータ配送手段42が偏 号化対象データを作成する暗号化対象データ作成手段も 【0046】暗号化対象データ作成装置4としては、暗 1と、作成した暗号化対象データをデータ送信装置1の

的には、通常のテキストエディターや既存のWMデータ ンで配送する手段等をとることができる。

信装置の秘密銀保管手段に配送するとともに、生成した に固有のユーザ秘密鍵及びユーザ公開鍵を生成するユー は、後で説明する。ユーザ鍵生成装置5は、各ユーザ毎 ザ鍵生成手段51と、生成したユーザ秘密鍵をデータ交 【0048】暗号化対象データのデータ構造について

【0041】すなわち、プラグインを利用する場合、陥

ステムの全体構成を示す。

【0045】この成により、YMTプラウザ200と復

体的な実現方法としては、例えば、暗号化対象データを エアが実装されたコンピュータ (パソコンやワークステ ーション)が利用できる。またデータ配送手段42の具 フロッピーディスクなどの記録媒体に記録してオフライ (ホームページなど) を作成するための市販のソフトウ 【0047】暗号化対象データ作成装置4として、具体

ユーザ公開鍵を、データ暗号化装置の公開健保管手段に 的に安全な媒体に記録してオフラインで配送する手段 ーザ鍵配送手段としては、例えば、ICカードなどの物理 とが利用できる。またユーザ秘密観を配送するためのユ プログラムを実装したパソコンやワークステーションな 配送するためのユーザ酸配送手段52を備えている。ユ - ザ独生成装置5としては、具体的には、ユーザ観生成

と証明會をネットワークを利用してオンラインで電子的 証明書を、フロッピーディスクなどの記録媒体に記録し 送する手段や、認証局と呼ばれる公的機関にユーザ公開 公開鍵を配送するためのユーザ鍵配送手段としては、例 送する手段などを利用することができる。また、ユーザ **暗号化されたユーザ秘密盤をネットワークを利用して配** の記録媒体に記録して配送する手段や、パスワード等で 健略号方式により略号化した上でフロッピーディスク等 や、ユーザ協密鍵をユーザのパスワード等を用いて共通 てオフラインで配送する手段や、または、ユーザ公開銀 鍵に対する証明的の発行を受けた上で、ユーザ公開鍵と えば、1Cカードなどの物理的に安全な秩体に記録して配 に配送する手段などを利用することができる。

成も可能である。 で実現することも可能である。例えば、ユーザの利用す について説明したが、これらの製匠を買じコンピュータ 生成装置5は、それぞれ異なる装置として実現する場合 夕受信穀四2、暗号化対象データ作成穀四4、ユーザ題 夕受信装匠と、ユーザ鎧生成装匠の各機能を持たせる精 るコンピュータに、暗号化対象データ作成装置と、デー 【0049】なお、ここでは、データ送信袋匠1、デー

対象データを組み込まれた命令に従って暗号化した結果 処理命令が狙み込まれた暗号化対象データと、この暗号 として得られる暗号化データのデータ構造について説明 遺」次に、本返施の形態で扱う、時号処理を含むデータ 【0050】「暗号対象データ及U暗号化データの構

いて作成する場合について説明するが、他の記述習話に 略号化データとして、WMデータの原準的な記述目語で **協力いて同様に作成することも可能である。** ある、HTML(Hypertext Markup Language) 曽語に塩グ 【0051】なお、ここでは、暗号化対象データおよび

時号化対象データ01は、通常の肝処君語で記述された 号化範囲指定命令61や、この暗号化対象データの受信 データ本体DOに、暗号化するデータ範囲を指定する暗 対象データの構造例である。図5 (1)に示すように、 追加された構造をとる。 者を指定する受信者指定命令(2などの暗号処理命令時が 【0052】図5(1)は、本実施の形照で扱う暗号化

に、暗号化データD2は、復号する範囲を指定する復号 徳囲指定命令(3や、この母や化データの交供者が復身す 暗号化データの僻浩例である。図5 (2) に示すよう 【0053】また、図5(2)は、本実施の形態で扱う

-7-

C4などの時号処理命令時が追加された構造をとる。 る際に利用する壁情報を指定するための壁情報指定命令

することが可能となる。 指定命令により、データ提供者は、提供するデータに対 うち昭号化する領国を指定する命令である。母母化領国 おいて必ず指定される命令であり、略号化対象データの において、母母化類国指定命令は、母母化対象データに に組み込まれる時号処理命令群の既について示す。 図 6 して、必要に応じて、必要な範囲だけを明号化して扱り 【0054】図6に、暗号対象データ及び暗号化データ 【0055】また、受信告指定命令は、必要に応じて指

|正しく很号できるように暗号化対象データを鳴号化す は、この受信者指定命令により指定された受信者のみか る。データの暗号化の群類類成については後で説明す 者をあらかじめ指定する命令である。受信者指定命令が 指定された場合、データ暗号化数四のデータ暗号化手段 定される命令であり、暗号化対象データを受信する受信

供するデータが、復号できないように朝御することが可 ることにより、あらかじめ指定した受信者以外には、提 【0056】データ提供者は、受信者指定命令を利用す

命令とは異なり単なるコメントとして扱われる(以下、 囲まれたデータを暗号化することを指定する。なお、こ 化したり、指定した受信のみが復号できるように暗号化 とにより、既存のWRWサーバやブラウザに影響を与える この命令をコメント命令と称する)。 したがって、既存 こで、HTML 包括では、文字列"<!***-->は、通常の SECRET->で呼号化模国の国始と終了を指定し、これらで ことなく、データを必要に応じて必要な範囲のみを暗号 頼り当てている。このようにコメント命令を利用するこ 命令は、コメントとして無扱され、MMTプラウザや、MMT のWMアラウザや、WMサーバにおいて、時号代徳囲指定 は、次のような文字列<!--BEGIN SECRET->と、<!--END するための命令を暗号化対象データに組み込むことが可 利用し、それぞれ特定の文字列を所定の暗号処理命令に ように他の母号処理命令も、HTML哲語のコメント命令を サーバに影響を及ぼすことはない。同様に、図9に示す 【0057】また、暗号化短囲指定命令は、具体的に

号手段25の辞組構成について説明する。 町号化手段14と、データ受信装置2におけるデータ復 静細博成」ここでは、データ送信装置1におけるデータ 【0058】「データ暗号化手段及びデータ很号手段の

を用いて、共通健略号方式により暗号化対象データのう 1と、データ歴生成手段141にて生成されたデータ製 であるデータ鍵を生成するためのデータ鍵生成手段14 は、暗号化対象データを暗号化する際に利用する、乱数 図4に示す。図4に示すように、データ時号化手段14 【0059】まず、データ町号化手段14の群期構成を

> 銀暗号化手段144と、暗号化された暗号化対象データ て、公園銀階号方式により、データ銀を暗号化する公開 から、受信者指定命令、もしくは、データ受信装置から 哲手段143において保管されているユーザ公開鍵の中 哲するユーザ公開健保管手段143と、ユーザ公開健保 通銀時号化手段142と、各ユーザのユーザ公開錠を保 ち殴号化範囲指定命令で指定された範囲を磨号化する共 略号化データ生成手段145より構成される。 化されたデータ酸を指定する酸情報指定命令を追加する に、復号する範囲を指定する復号範囲指定命令や、暗号 ザ公開鍵を取り出し、取り出されたユーザ公開鍵を用い 受信した受信者識別情報により指定された受信者のユー

【0060】 データ復号手段13の詳細構成を図4

同じ共通健暗号方式を用いて、暗号化データのうち復号 段254より構成される。 範囲指定命令で指定された範囲を復号する共通路復号手 鍵を用いて、データ暗号化手段において利用したものと て復身する公園銀復号手段253と、復号されたデータ 手段において利用したものと同じ公開酸暗号方式を用い 密顔を用いて、暗号化されたデータ顔を、データ暗号化 秘密避保管手段 2 5 2 において管理されているユーザ協 手段254に渡すための暗号化データ解析手段251 のうち彼号範囲指定命令で指定された範囲を共通観復号 データ鍵を公開鍵復号手段253に渡し、暗号化データ た暗号化されたデータ鍵を取り出し、この暗号化された 段25は、暗号化データから銀情報指定命令で指定され と、ユーザ秘密観を保管する秘密銀保管手段252と、 (2) に示す。図4 (2) に示すように、データ彼号手

いついた奴団する。 【0061】「詳細な動作」次に、本実施の形態の動作

の役、個々の処理の詳細動作について説明する。 [0062]まず、全体の動作販路について説明し、そ

【0063】(1) 本実施の形態全体の動作販路

の全体の助作概略を示すフローチャートである。 図7は、本実施の形態におけるデータ暗号通信システム 【0064】図7に示すように、本実施の形態は、新規

のユーザが利用を開始するときに行うユーザ鍵生成処理 取得するときに行うデータ取得処理(ステップS30 処理(ステップS200)と、ユーザが、提供データを (ステップS1 0 0)と、データの提供者が提供データ (暗号化対象データ)を作成するときに行うデータ作成

るデータ受信装団に、またユーザ公開鍵を、データ送信 を生成し、生成したユーザ協密鍵をそのユーザの利用す ユーザ協密鍵と、ユーザ協密鍵に対応するユーザ公開鍵 鍵生成装匠を利用して行う。 具体的には、各ユーザ用の ユーザ自身、もしくは、本システムの管理者が、ユーザ 装囮に配送するなどの処理を行う。 【0065】 ここでユーザ胎生成処理 (S100) は、

【0066】 データ作成処理(S200) は、データ類

対象データを、データ送信装置に配送するなどの処理な 供者が、暗号化対象データ作成装置を利用して行う。具 体的には、暗号化対象データを作成し、作成した暗号化

から、そのデータ要求情報に対応する暗号化された暗号 化データを復号し取得するなどの処理を行う。 化対象データ (暗号化データ) を受信し、受信した暗号 タ要求情報をデータ送信装置に送信し、データ送信装置 提供データ(暗号化対象データ)の送信を要求するデー ーザが、自分のデータ受信装置を利用して、取得したい が、データ受信装置を利用して行う。具体的には、各コ

ザ公開發保管手段により、ユーザ公開鍵を保管する(ス ユーザ鍵配送手段により、生成したユーザ秘密鍵を、第 り、各ユーザ用に、ユーザ秘密盤とそのユーザ秘密盤に テップS150)。 ようにデータ送信装団のユーザ公開健保管手段に配送し り、生成したユーザ公開鍵を、第三者に改ざんされない し(ステップS130)、また、ユーザ銀配送手段によ いて、ユーザ秘密銀保管手段によりユーザ秘密盤を保管 段に配送し(ステップS120)、データ受信装置にお 三者に窓見しないようにデータ受信装匠の秘密健保管手 対応するユーザ公開題を生成し(ステップSIIO) は、ユーザ競生成装置において、ユーザ競生成手段によ (ステップS140)、データ送信装匠において、ユー [0069] 図8に示すように、ユーザ鍵生成処理で

的な手段としては、ユーザ公開観に、公的な認証局の発 第三者により改ざんされないように配送するための具体 するなどの手段が利用できる。また、ユーザ公開鍵が、 配送するか、または、ICカードを利用して手渡して配送 渋しで配送するか、ネットワークを介してオンラインで 方式で略号化した後、フロッピーディスクに記録して手 配送するための具体的な手段としては、ユーザ秘密器 クやICカードに記録して手渡して配送するなどの手段が 行した証明啓を添付して転送するか、フロッピーディス を、ユーザの指定したパスワードを用いて、共通銀駐号

図9は、データ作成処理の詳細動作を示すフローチャー

略号化対象データ作成装置において、略号化対象データ 作成手段により、暗号化範囲指定命令や受信者指定命令 などを組み込んだ暗号化対象データを作成し(ステップ

【0067】 データ取得処理(S300) は、各ユーサ

【0068】(2) ユーザ鍵生成処理(S100)の

図8は、ユーザ競生成処理の辞細動作を示すフローチャ

【0070】ユーザ秘密融が第三者に露見しないように

【0071】(3) データ作成処理(S200)の群

[0072] 図9に示すように、データ作成処理では、

データを、データ送信装匠のデータ保管手段に配送し 210)、データ配送手段により、作成した暗号化対象 銀データを保管する(ステップ220)。 (ステップ220)、データ送信装匠において、暗号化片

な寒現方法としては、暗号化対象データをフロッピーな どの記録媒体に記録して手渡した配送するなどの手段が [0073] 暗号化対象データを配送するための具体的

【0074】 (4) データ取得処理 (S300)の群

まず、データ送信装置を、WMサーバとCGIプログラム は、この場合のデータ取得処理の群組動作を示すフロー で構成する場合の詳細動作について説明する。図13 で、データ受信装置を、WMプラウザと復号プラグイン

若識別情報で指定された受信者のみが復分できるように 時号化対象データを、受信者指定命令、もしくは、受信 報をデータ送信穀匠に送信し(ステップS320)、デ 定を受け取り (ステップS310)、データ通信手段に は、まず、テータ受信装匠のMMプラウザにおいて、ユ 信装置に送信し(ステップS360)、データ受信装置 昭号化して、昭号化データを作成し(ステップS35 報と、オプションとして受信者を指定する受信者煥別的 などのためにデータ出力手段に渡す (ステップ539 段により、復号された暗号化データを、ディスプレ表示 し(ステップS370)、データ彼号手段により、吓号 において、データ通信手段により、暗号化データを受信 ップS340)、データ暗号化手段により、取得された タ要求情報に対応する暗号化対象データを取得し(ステ ップS330)、データ取得手段により、受信したデー より、データ要求情報と受信者識別情報を受信し(ステ ータ送信装匠のWMサーバにおいて、データ通信手段に より、指定されたデータの送信を要求するデータ要求情 ーザ入力手段により、ユーザから取得したいデータの指 化データを復号し(ステップS380)、データ処理手 0)、データ通信手段により、暗号化データをデータ受 【0075】図10に示すように、データ取得処理で

命令の組み込まれたデータにおいて、その命令を実行す 接入力する方法や、収得したいデータのURLを指定する orm Resource Location)と呼ばれる取得したいデータの が収得したいデータを指定する方法としては、URL(Unit ることによって行う方法などを利用できる。 アドレス情報(データの保管場所を指定する情報)を直 【0076】ここで、ステップS310においてユーザ

0) の辞組な動作を示すフローチャートである。 における暗号化対象データの暗号化(ステップS35 [0077] また、図11(1)は、データ暗号化手段

手段では、データ競生成手段により、データ観を生成し 【0078】図11(1)に示すように、データ時身化

手段に保管されている各ユーザのユーザ公園館の中か 範囲指定命令で指定された範囲を闘号化し(ステップS したデータ酸を用いて、暗号化対象データのうち暗号化 公開鍵を利用して、公開鍵時号化し(ステップS35 された受信者のユーザ公開館を取得し、取得したユーザ を狙み込んだ町号化データを作成する(ステップ35 夕館を指定する時号観情報指定命令と復号範囲指定命令 3)、昭号化データ作成手段により、昭号化されたデー ら、受信者指定命令、もしくは、受信者は別情報で指定 352)、公園健康号化手段により、ユーザ公園健保管 (ステップS351)、共通短時身化手段により、生成

な動作を示すフローチャートである。 おける町号化データの復号(ステップS380)の辞載 【0079】また、図11(2)は、データ復号手段に

取得し (ステップ5381)、公開競役号手段により、 段では、暗号化データ解析手段により、暗号化データか 号された暗号化データを収得する (ステップS38 ユーザ秘密題保管手段に保管されたユーザ秘密題を用い ら既情報指定命令で指定された暗号化されたデータ鍵を 用して暗号化データを復号し(ステップS383)、 復 2)、共通の復号手段により、復号されたデータ母を利 て、町号化されたデータ壁を復号し(ステップS38 【0080】図11(2)に示すように、データ復号手

信者識別情報を送信する必要はない。 を組み込むことにより、暗号化対象データの受信者を指 定する場合は、データ受信装置からデータ送信装置に受 【0081】なお、暗号化対象データに受信者指定命令

号化プロキシで、データ受信数囚を、WMプラウザと復 示すフローチャートである。 る。図12は、この場合のデータ取得処理の詳細動作を **导プロキシで構成する場合の辞担動作について説明す** 【0082】次に、データ送信袋匠を、MMサーバと時

は、まず、データ受債装置のMMVブラウザにおいて、ユ テップS440)、データ通信手段により暗号化対象デ 報を、データ送信裝位に送信し (ステップS420)、 報と、オプションとして受信者を指定する受信者識別情 定を受け取り (ステップS410)、データ通信手段に ーザ入力手段により、ユーザから取得したいデータの指 化手段により、取得された暗号化対象データを、受信者 対象データを受信し(ステップS460)、データ環号 昭号化プロキシにおいて、データ通信手段により暗号化 ータを暗号化プロキシに送信し(ステップS450)、 一夕要求情報に対応する暗号化対象データを取得し(ス テップS430)、データ取得手段により、受信したデ により、データ要求情報と受信者識別情報を受信し(ス データ送信数位のWMサーバにおいて、データ通信手段 より、指定されたデータの送信を要求するデータ要求情 【0083】図12に示すように、データ収得処理で

> S510)、竹帽ブラウザのデータ通信手段により、復 された暗号化データをRMYプラウザに送信し(ステップ スプレ表示などのためにデータ出力手段に渡す(ステッ 号された暗号データを受信し(ステップS520)、デ 90)、データ復身手段により、暗号化データを復号し 通信手段により、暗号化データを受信し(ステップS4 0)、データ受信装置の復号プロキシにおいて、データ 町号化データを復号プロキシに送信し(ステップS48 作成し(ステップS470)、データ通信手段により、 者のみが似号できるように暗号化して、暗号化データを 指定命令、もしくは、受信者識別情報で指定された受信 ータ処理手段により、復号された暗号化データを、ディ (ステップS500)、テータ通信手段において、復号

信装置にて、受信した暗号化データを復号して取得する 当の暗号化データをデータ受信装置に送信し、データ受 位にて、データ受信装置からの送信要求に対応して、数 あらかじめ暗号化データを拮納しておき、データ送信袋 場合について説明する。 【0084】(実施の形態2) 大に、データ送信装置に

に、本システムの辞組な動作について説明する。 【0085】まず、システムの構成について説明し、次

するネットワーク3と、暗号化データ作成装置6と、ユ る。図13に示すようにデータ暗号通信システムは、デ 憩におけるデータ暗号通信システムの概略構成器であ システム構成について説明する。図13は、本実施の形 ータ送信装置1と、データ受信装置2と、これらを接続 - ザ競虫成装団 5 によって構成される。 【0086】「システムの構成」本実施の形態の全体の

生成教団の構成は、実施の影照1と同じものが利用でき るので、ここでは説明を省略する。 【0087】ここで、データ受信装団、及び、ユーザ図

報を受信しそのデータ要求情報に対応した暗号化データ 化データを保管するためのデータ保管手段13で構成さ ータ通信手段に渡すためのデータ取得手段12と、暗号 をデータ受信装置2に送信するためのデータ通信手段1 らのデータ要求情報及びオプションとして受信者識別情 -夕保管手段13から取り出し、この略号化データをデ 1 と、上記データ要求情報に対応する暗号化データをデ 【0088】データ送信装置1は、データ受信装置2か

> を取得するときに行うデータ取得処理(ステップS30 成処理(ステップS200)と、ユーザが、提供データ

(応号化データ)を作成するときに行う暗号化データ作

WMIプラウザ間の概単過倍プロトコルであるHTTPプロト WMサーバの備えるデータ通信手段11が、WMサーバと やワークステーションなど) が利用できる。この場合、 ationサーバなど) を実装したコンピュータ (パソコン 手段を備えた、既存のWWN(World Wide Web)サーバ(例 上記データ通信手段と、データ取得手段と、データ保管 コルに協力いてデータ適信を行う。 えば、Netscape Communications社のNetscape Communic 【0089】データ送信装置1としては、具体的には、

> **格成については実施の形態1の場合と同じであるので数** 成された各ユーザのユーザ公開鍵を保管するための公開 化手段には、図示していないが鍵生成装置 5 によって生 暗号化データをデータ送信装置のデータ保管手段13に 号化データを生成するためのデータ暗号化手段62と、 信者指定命令にて指定された受信者向けに暗号化して暗 対象データを作成する暗号化対象データ作成手段61 明は省略する。 鎮保管手段を備えている。データ暗号化手段14の詳細 配送するデータ配送手段63を備えている。データ暗号 と、作成した暗号化対象データを暗号化対象データを受 【0090】暗号化データ作成装置6としては、暗号化

ン)が利用できる。 実装されたコンピュータ (パソコンやワークステーショ 7、及び、データ暗号化手段を実現するプログラムとが ームページなど)を作成するための市販のソフトウエ は、通常のテキストエディターや既存の解析データ(ホ 【0091】暗号化データ作成装置として、具体的に

手段等をとることができる。 イスクなどの記録媒体に記録してオフラインで配送する 法としては、例えば、暗号化対象データをフロッピーデ 【0092】またデータ配送手段42の具体的な実現方

タ傑造については、実施の形態1の場合と同じであるの 【0093】暗号化対象データ及び暗号化データのデー

こついた試圧する。 [0094] 「辞細な動作」次に、本実施の形態の動作

[0095]まず、全体の動作販路について説明し、

ユーザが利用を開始するときに行うユーザ鍵生成処理 動作既略としては、実施の影照1と同様であり、新規の 本実施の形団におけるデータ暗号通信システムの全体の の後、個々の処理の詳細動作について説明する。 (ステップS100)と、データの提供者が提供データ 【0096】(1) 本実施の形態全体の動作展局

体的には、各ユーザ用のユーザ秘密観と、ユーザ秘密観 実施の形態1と同様に、ユーザ自身、もしくは、本シス 鍵をそのユーザの利用するデータ受信装置に、またユー テムの管理者が、ユーザ壁生成装置を利用して行う。具 ザ公開鍵を、データ送信装置に配送するなどの処理を行 に対応するユーザ公開鍵を生成し、生成したユーザ秘密 【0097】 ここでユーザ競生成処理(S100)は、

憩 1 と異なり、データ提供者が、暗号化データ作成装置 [0098] データ作成処理 (S200) は、実施の形

【0099】具体的には、暗号化対象データを作成し

に配送するなどの処理を行う。 作成した暗号化対象データを暗号化し、データ送信装的

る時号化データを受俗し、受信した時号化データを復号 送信を要求するデータ要求惰報をデータ送信装置に送信 を利用して、取得したい提供データ(暗号化データ)の 行う。具体的には、各ユーザが、自分のデータ受信袋医 隠 1と異なり、各ユーザが、データ受信装置を利用して し、データ送信装低から、そのデータ要求情報に対応す し取得するなどの処理を行う。 【0100】データ取得処理(S300) は、実施の影

【0101】(2) ユーザ超生成処理(S100)の

ユーザ鍵生成処理の動作は、疾歯の形態1の場合と同じ であるので説明は省略する。 [0102] (3) データ作成処理 (S200) の群

図14は、データ作成処理の群組動作を示すフローチャ

作成手段により、暗号化範囲指定命令や受信者指定命令 210)、暗号化対象データを、受信者指定命令で指定 は、暗号化データ作成数位において、暗号化対象データ 技匠において、暗号化データを保管する(ステップ24 より、作成した暗号化対象データを、データ送信效性の 化データを作成し(ステップ220)、データ配送手段に された受信者のみが復身できるように時号化して、時号 などを組み込んだ時号化対象データを作成し(ステップ データ保管手段に配送し(ステップと30)、データ送信 【0103】図14に示すように、データ作成処理で

形態 1 の場合と同様であるので説明は省略する。 タの時号化(ステップS220)の群組な動作は実施の 【0104】データ暗号化手段における暗号化対象デー

を利用してオンラインで配送するなどの手段が利用でき **媒体に記録して手渡しで配送する方法や、ネットワーク** 現力法としては、暗号化データをフロッピーなどの記録 【0105】暗号化データを配送するための具体的な実

【0106】 (4) データ取得処理 (S300) の律

まず、データ受信装匠を、WMプラウザと復号プラグイ は、この場合のデータ取得処理の辞細動作を示すフロー ンで構成する場合の舞蹈動作について説明する。図15

は、まず、データ受信装匠のWMプラウザにおいて、ユ 7サーバにおいて、データ通信手段により、データ要求 より、指定されたデータの送信を吸水するデータ吸水倍 定を受け取り (ステップS 3 1 0) 、データ通信手段に 類を送信し(ステップS320)、データ送信数配のM ーザ入力手段により、ユーザから取得したいデータの指 【0 1 0 7】図1 5 に示すように、データ取得処理で

にデータ出力手段に渡す(ステップS380)。 復身された暗号化データを、ディスプレ表示などのため 復号し(ステップS370)、データ処理手段により、 プS360)、データ復号手段により、暗号化データを 信し(ステップS350)、データ受信装置において、 タ通信手段により、暗号化データをデータ受信装置に送 する時号化データを取得し (ステップS340)、デー データ取得手段により、受信したデータ要求情報に対応 情報と受信者識別情報を受信し(ステップS330)、 データ通信手段により、暗号化データを受信し(ステッ

場合と同様であるので説明は名略する。 号(ステップS370)の群相な動作は実施の形態1の 【0108】データ従号手段における時号化データの復

示すフローチャートである。 る。図16は、この場合のデータ取得処理の群曲動作を 復りプロキッス構成する場合の評価動作について説明す 【0 1 0 9】次に、データ受信装置を、MMブラウザと

り、役号された暗号化データを、ディスプレ表示などの を受信し(ステップS490)、データ処理手段によ 0)、データ通信手段において、復号された暗号化デー **号手段により、暗号化データを復号し(ステップS47** 略号化データを受信し(ステップS 4 6 0)、データ很 松田の彼母プロキシにおいて、アータ道館年段により、 号プロキシに送信し(ステップS450)、データ受作 ータ要求情報に対応する暗号化データを取得し(ステッ テップS430)、データ取得手段により、受信したテ により、データ要求情報と受信者識別情報を受信し(ス 報を、データ送信装位に送信し (ステップS420)、 完を受け取り (ステップS410)、データ通信手段に は、まず、データ受信装匠のWMブラウザにおいて、ユ ためにデータ出力手段に波す (ステップ5500)。 ラウザのデータ通信手段により、復身された暗号データ プS440)、データ通信手段により時号化データを復 データ送信装匠のWMサーバにおいて、データ通信手段 より、指定されたデータの送倒を要求するデータ要求情 タをIMWブラウザに送信し(ステップS480)、IMWフ ーザ入力手段により、ユーザから取得したいデータの指 【0110】図16に示すように、データ取得処理で

UMMを利用する場合について説明したがそれに限るも では、データの送信及びデータの受信に、mmサーバ及 【0112】また、データとして、HPA国語に基づいて 【0111】なお、実施の形成1、及び、実施の形成2

いて規則したが、それに限るものではない。 各種データ処理の命令が組み込まれたデータの場合につ 場合について説明したが、それに限るものではない。 利用したデータ鍵の暗号化に公開鍵暗号方式を利用する の時号化に共通健康身方式を利用し、データの暗号化に 【0113】また、データの暗号化手段として、データ

> むことにより、暗号化対象データは、暗号化範囲指定命 暗号化する範囲を指定する暗号化範囲指定命令を組み込 したり、一部はすべての受信者に視聴させることが可能 に応じて、暗号化対象データの重要な部分のみを暗号化 令で指定された範囲のみ暗号化される。このため、必要 【発明の効果】本発明によれば、暗号化対象データに、

あらかじめ受信者を限定することが可能となる。 号化することが可能となる。すなわち、必要に応じて、 データを、指定した受信者以外は復身できないように暗 する受信者指定命令を組み込むことにより、暗号化対象 【0115】また、暗号化対象データに、受信者を指定

定された範囲のみを暗号化するためのデータ暗号化手段 号送信を行うデータ暗号装置が提供可能となる。 のITITサーバを変更することなく利用した、データの暗 行うためのデータ通信手段とを備えた暗号化プログラム パと、暗号化対象データのうち暗号化範囲指定命令で指 とを実装したコンピュータで構成することにより、既存 とMMサーバ及びMMプラウザとの国でデータの送受信を 【0 1 1 6】また、特に、データ送信装置を、NYMサー

変更することなく利用した、暗号化データの復号受信を 通信手段とを備えた復号プログラムとを、実装したコン ラウギと、暗号化データのうち資号領囲指定命令な指院 行うデータ暗号装置が提供可能となる。 ピュータで構成することにより、既存のBMTプラウザを 及びWMアラウザとの間でデータの送受信を行うデータ された範囲のみを復号するデータ復号手段と8977サーバ [0117] 同様に、特に、データ復号装置を、RMTプ

やプラウザに影響を与えることがない。 用して暗号処理命令を定義するため、既存の問的サーバ 【0 1 1 8】また、特に、HTML台語のコメント命令を利

【図酒の餌単な説明】

4の金体構成図 【図1】本発明の実施の形態1のデータ暗号通信システ

ータ暗号通信システムの全体構成図 【図3】暗号化プロキシ及び復号プロキシを利用したテ 【図2】データ送信装置及びデータ受信装置の構成図

【図4】データ暗号化手段及びデータ復号手段の詳細構

近例を示す凶 【図5】 暗号化対象データ及び暗号化データのデータ模

【図6】昭号処理命令の一覧を示す図

【図1】 全体の動作概略を示すフローチャート

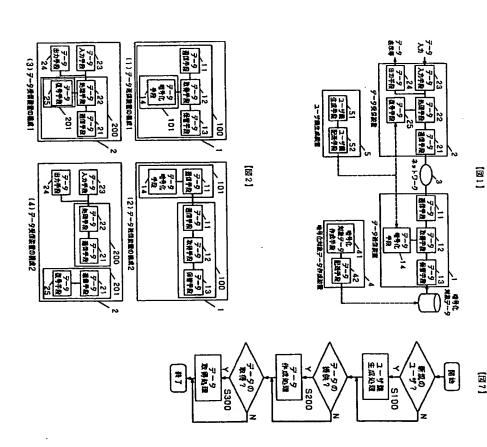
【図8】ユーザ鍵生成処理のフローチャート 【図9】 データ作成処理のフローチャート

【図11】データ暗号化手段及びデータ復号手段の処理 【図10】データ取得処理のフローチャート

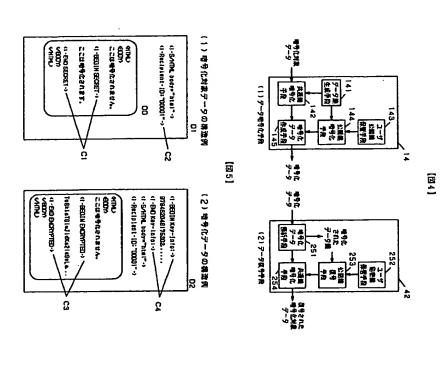
- タ取得処理のフローチャート 【図】2】 晴号化プロキシ及び復号プロキシ利用時のテ

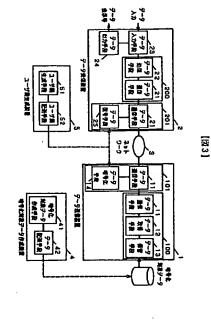
のフローチャート

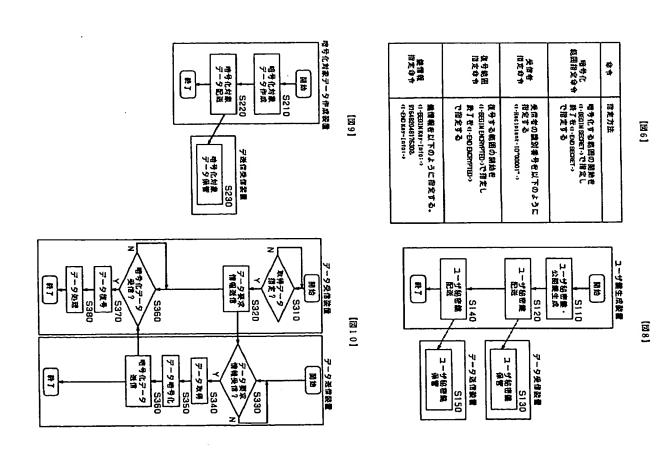
テムの全体構成図 ーチャーケ 【図13】本発明の実施の形態2のデータ暗号通信シス Ⅰ データ送信装置 【図16】復号プロキシ利用時のデータ取得処理のフロ 【図15】データ取得処理のフローチャート 【符号の説明】 【図14】データ作成処理のフローチャート 25 データ復号手段 201 復身プロキシ 200 WWアラウザ 101 時号プロキシ 1 4 5 ユーザ競生成数回 データ受信装置 暗号化対象データ作成数団 データ暗号化手段



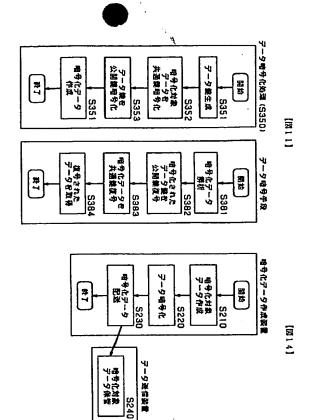


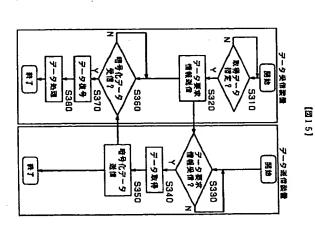






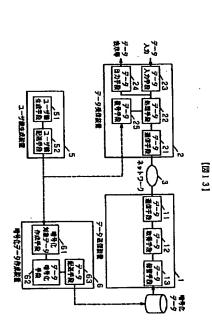
- 15 -





[图12]

546 7-920 9347 7-9490 7-9490



- 18 -

- 17 -

停踢平11-215122

[四16]

フロントページの投き

テム名古恩研究所内

(72)発明者 西族 丘 愛知県名古昭市中区栄2丁目6番1号白川 ビル別館5階 株式会社松下電器情報シス

- 19 -

(72)発明者 小野 黄敏 愛知県名古盟市中区衆2丁目6番1号白川 ビル別館5階 株式会社松下電器情報シス テム名古屋研究所内

